Themenbereich	Beschlußvorlage Software Anschaffung 0 EUR: Basisdemokratische Beteiligung der Mitglieder durch Consul Instanz
Paragraf	
Antragsteller	Helmut Grunst
Mitgliedsnummer	20025788
Kontakt	Helmut Grunst, Hochgartenstraße 3, 84091 Attenhofen
Gegenstand / Thema	Basisdemokratische Beteiligung durch Consul Instanz für LV dieBasis Bayern
abstimmungsfähiger Wortlaut	Der Landesvorstand Bayern wird beauftragt, die basisdemokratische Software Consul anzuschaffen und den Mitgliedern zu Verfügung zu stellen.
Begründung	**Damit wird nach drei Jahren endlich das Versprechen eingelöst, den Mitgliedern die Möglichkeit einer umfassenden Mitgestaltung zu eröffnen. Die basisdemokratische Software Consul ermöglicht den Mitgliedern auf einer Plattform gleichberechtigt zu diskutieren, Vorschläge zur Abstimmung einzubringen und darüber endgültig abzustimmen. Damit kommt der Schwarm ins Wirken. Damit treffen die Vorstände Entscheidungen nicht mehr ganz alleine, sondern können sich auf den Schwarm berufen. Das stärkt sowohl die Vorstände als auch die Basis, die aktiv einbezogen wird.** Consul Democracy ist ein umfassendes Abstimmungs- und Vorschlagssystem, das nicht nur einfache Abstimmungen ermöglicht, sondern auch eine breite Palette von Modulen bietet, um den gesamten politischen Entscheidungsprozess abzudecken. Im Folgenden werden die verschiedenen Module von Consul näher erläutert: 1. Diskussion: Das Diskussionsmodul ermöglicht es den Nutzern, ihre Ideen und Meinungen auszutauschen und in einen konstruktiven Dialog zu treten. Es bietet eine Plattform

erhalten. Wenn ein Vorschlag genügend Zustimmung erhält, kann er ohne weitere administrative Abstimmung direkt zur Abstimmung freigegeben werden. Dies ermöglicht eine effiziente Umsetzung von Ideen, die von der Gemeinschaft unterstützt werden.

3. Administrative Abstimmung: Neben den direkten Abstimmungen über Vorschläge gibt es auch die Möglichkeit einer administrativen Abstimmung. Dieses Modul ermöglicht es den Administratoren, wichtige Entscheidungen zu treffen, die nicht direkt von der Gemeinschaft abgestimmt werden müssen. Dies kann beispielsweise bei komplexen oder zeitkritischen Angelegenheiten der Fall sein. Die administrative Abstimmung gewährleistet eine effektive Entscheidungsfindung und ermöglicht es, den politischen Prozess reibungslos fortzusetzen.

4. Gesetzgebungsentwicklung: Das Modul zur Gesetzgebungsentwicklung ermöglicht es den Nutzern, aktiv an der Erstellung und Überarbeitung von Satzungen mitzuwirken. Es bietet eine Plattform, um Satzungsvorschläge einzubringen, zu diskutieren und zu bewerten. Dies fördert eine transparente und partizipative Satzungsgebung und ermöglicht es den Menschen, ihre Stimme in den politischen Prozess einzubringen.

5. Budgetverwaltung: Das Modul zur Budgetverwaltung ermöglicht es den Bürgern, Vorschläge für die Verwendung von zugewiesenen Geldern einzureichen und zu bewerten. Dies schafft Transparenz und ermöglicht es den Mitgliedern, Einfluss auf die Prioritäten und Ausgaben des Vorstands zu nehmen. Durch eine breite Beteiligung an der Budgetverwaltung wird sichergestellt, dass die Bedürfnisse und Wünsche der Mitglieder berücksichtigt werden.

Consul Democracy bietet somit eine umfassende Plattform, die alle Aspekte des politischen Entscheidungsprozesses abdeckt. Mit seinen verschiedenen Modulen ermöglicht es den Bürgern, sich aktiv einzubringen, Ideen auszutauschen, Vorschläge zu machen, Satzungen zu entwickeln und die Verwendung von Geldern mitzugestalten. Dies fördert eine partizipative Demokratie und trägt zu einer transparenten und effektiven Führung des Organs Landesvorstand bei.

Beschlußvorlage:

Testbericht; Überprüfung der Kommunikation von Consul vom 26.12.2023, 16:00 – 27.12.2023, 16:00

Autoren: Hermann, stefan hubschmid

Zusammenfassung

Wir testen Consul, eine Diskussions- und Abstimmungssoftware. Um die Datensicherheit zu klären, haben wir vom 26.12.2023, 16:00 – 27.12.2023, 16:00 einen Sniffer – Test gemacht um den Datenverkehr von Consul zu überprüfen. Eine kleine Gruppe hatte während der Testphase Consul möglichst umfassend genutzt. Gleichzeitig haben wir mit einem Programm alle IP – Adressen aufgezeichnet, welche einen Datenverkehr mit dem Server hatten. Nach Testabschluss wurden alle IP – Adressen überprüft. Insgesamt hatten 15 IP – Adressen mit dem Server kommuniziert. 9 davon konnten wir entweder den Testern oder Serverinternen IP – Adressen zuordnen. 6 IP – Adressen mussten wir genauer untersuchen. 1 Kontakt konnte einem Tester zugeordnet werden, dessen Cache dazu geführt hatte, dass ein IP – Wechsel nicht erkannt wurde. 2 Kontakte konnten wir einem Serverupdate zuordnen. 1 Kontakt einer Zertifikatsüberprüfung. 1 Kontakt war zu einer Sitemap von Google, was üblich ist um den Suchmaschinen das Crawlen zu erleichtern. 1 Kontakt war vermutlich nur ein Portscan.
Keine der übertragenen Daten und Kontakte weist auf eine Kommunikation mit externen Diensten hin, welche wir als kritisch für die Datensicherheit werten konnten. Aufgrund des Tests können wir keine Überwachung der Software durch dritte und keine unbefugte Kommunikation, mit relevantem Datenverkehr, zwischen Consul und anderen Diensten feststellen. Es wurden keine Kontakte mit WEF – verbundenen Diensten oder Seiten festgestellt.

Hintergrund

Viele Menschen und Gruppen möchten eine hierarchiefreie Selbstorganisation der Menschen stärken und geeignete Strukturen dazu einführen. Unsere Gruppe aus verschiedenen Organisationen (im Folgenden Tester genannt) testet zurzeit, ob die open source Software Consul[1] dazu genutzt werden kann. Consul ist ein bestehendes Programm und die Tester haben den Programmcode nicht vollumfänglich verstanden.
Um zu gewährleisten, dass Consul keine versteckte oder unbefugte Kommunikation mit anderen Diensten vollführt, wurde ein Testlauf gestartet und die Kommunikation von Consul mit anderen IP – Adressen überprüft (im Folgenden „Sniffer – Test“ genannt).
Zudem gab es Bedenken, dass Consul mit dem WEF kommunizieren könnte, da auf der Grundversion die Ziele der Agenda 2030 erscheint.

verschiedene Aktivitäten auf Consul durchzuführen.
Eine 24-Stunden – Messung dient der Kontrolle von zeitlichen Auslösern für eine versteckte Kommunikation. Die verschiedenen Aktivitäten dienten der Kontrolle ob verschiedene Ereignisse eine versteckte Kommunikation auslösen könnten.
Um den Datenverkehr zu erfassen wurde ein Proxmox-Server mit OpnSense Firewall VM[3] verwendet, welcher zwischen die externen und die interne IP – Adresse geschaltet wurde. Die Daten wurden als Zip – Datei von der Firewall heruntergeladen und mittels Wireshark in eine CSV – Datei umgewandelt[4].
Alle Tester wurden angewiesen ihre IP – Adressen zu prüfen[5] und zusammen mit ihren Aktivitäten in einer Onlinetabelle auf einem Faircloud - Account von Hermann einzutragen. Mittels dieser Tabelle wurden die IP – Adressen, welche durch die Firewall erhoben wurde, mit den IP – Adressen der Tester verglichen[6]. Alle restlichen IP – Adressen wurden versucht eindeutig zuzuordnen und falls nicht möglich, die kommunizierten Daten zu untersuchen und einzuschätzen.

Resultate

Es wurden durch die OpnSense Firewall VM insgesamt 15 IP – Adressen erhoben, welche miteinander kommuniziert haben. 9 davon konnten entweder Tester oder Serverinternen IP – Adressen zugeordnet werden.
1 IP – Adresse (31.16.251.102) stimmte mit den Aktivitäten eines Testers überein. Seine angegebene IP – Adresse (83.135.141.91) wurde hingegen zu dieser Zeit nicht gefunden. Eine Rückfrage ergab, dass die verwendete Seite https://www.wieistmeineip.de/ die alte IP – Adresse (83.135.141.91) im Cache des Browsers gespeichert hatte. Dadurch wurde nach einem Wechsel des Internetzugangs zwischen 2 Testsitzungen die neue IP – Adresse von der Seite nicht erkannt. Durch die übereinstimmenden Zeiten, die fehlende IP welche auf dem Protokoll angegeben wurde und den Fehler der Internetseite „wieistmeineip.de“ ist die Zuordnung der IP – Adresse zum Tester genügend nachgewiesen.
2 IP – Adressen (104.22.5.26 und 146.75.122.132) scheinen Updateanfragen bezüglich des Servers zu sein. In Kontakt nr. 54453[7] ist ersichtlich, dass die IP 104.22.5.26 zur Seite http://deb.nodesource.com/ führte, was zum Betriebssystem Debian gehört welches auf dem Server installierten ist. Es gab ferner keinen erheblichen Datenaustausch. Die IP 146.75.122.132 hatte laut Kontakt nr. 54414 versucht auf die Seite /debian/dists/bullseye/InRelease zuzugreifen und kann somit auch dem Debian – Update zugeordnet werden. Es gab einen minimalen Datenaustausch.
1 IP – Adresse (184.24.77.48) versuchte auf die Seite r3.o.lencr.org zuzugreifen (Nr. 54556). Die URL Lencr.org leitet auf https://letsencrypt.org/docs/lencr.org/ weiter, laut welcher die URL r3.o.lencr.org für die Überprüfung von OCSP – Zertifikaten zuständig ist. Der Datentransfer war nur sehr gering.
1 IP – Adresse (216.58.212.132) war eine Kontaktanfrage des Consul – Servers an Google.com. Dies konnten wir über infobyip.com feststellen[8]. Weiter wurde laut Kontakt – Nr. 54380 versucht auf

---

[2] Zu finden unter: https://88.99.25.57:34160/ -> diese Instanz wird auch für andere Zwecke benutzt und sich somit laufend verändern, Bildschirmaufnahme vom 29.12.2023 im Anhang: Bildschirmaufnahme_Consul_2023.12.29.jpg
[3] Einstellungen der Firewall siehe Anhang: Einstellungen der Firewall.jpg

1 IP – Adresse (79.124.60.138) hatte nur 3 Kontaktpunkte und scheint laut infobyip.com aus Bulgarien gekommen zu sein. Es fand kein ersichtlicher Datenaustausch statt.

Schlussfolgerung

Die Überprüfung der Kontakte mittels OpnSense Firewall VM ergab 15 IP – Adressen, welche während den 24 Stunden des Testlaufes mit der IP der getesteten Consulinstanz kommunizierten. 9 konnten durch die Protokollierung und den Serverinternen IP – Adressen direkt zugeordnet werden, 1 weitere nach Rücksprache mit einem Tester. Keine der 5 restlichen IP – Adressen deuten auf eine versteckte Kommunikation hin. 5 der 6 konnten eindeutig zugeordnet werden und haben einen erklärbaren Hintergrund. 1 IP hatte nur 3 Kontaktpunkte und ist von außen gekommen. Es könnte z.B. eine Anfrage eines Bot's oder Dienstes sein. Bei keinem Kontakt wurde eine erhebliche Menge an Daten ausgetauscht.
Eine Überwachung durch Dritte oder eine unbefugte Kommunikation von Consul mit anderen Diensten konnte nicht festgestellt werden. Somit wurde auch keine Kommunikation mit Diensten oder Seiten des WEF festgestellt.

Anmerkung

Alle Dateien sind für die Öffentlichkeit verfügbar und in einer Zip-Datei dem Bericht angeheftet. Wir stellen ebenfalls Testinstanzen von Consul für Snifftests zur Verfügung. Für Fragen oder zur Ausgabe der Daten stehen Helmut Grunst und Dante zur Verfügung.

Testergruppe Consul Stand 08.01.2024 Mitglieder im Test: 55
Mitglieder Basisdemokraten dieBasis
Mitglieder die-Basisdemokraten e.V.
Mitglieder H.e.l.f.a
Mitglieder Gemeinwohllobby
Mitglieder Freie Linke

EXERPT / Schlußwort Warum Consul:

1. Kein Vorstandsfilter / Gleichberechtigung von Vorstand / Mitglieder
… Schon allein die Entscheidung was aus Sicherheitsgründen für andere Software, die nur durch Vorstandsbewilligung genutzt werden darf ist per se ein FILTER durch Vorstand und Vorstandsbeauftragte durch Anwendung vorhanden.
2. Die Freiheit, dass ein jedes Mitglied frei entscheiden kann in Redaktion, Fragestellung, Abstimmungsart, ist die Waffengleichheit der Allgemeinverfügung durch Vorstand gegenüber.
3. Vorstand und Mitglieder brauchen nur den Zugang und den Internetbrowser, um Weltweit gleichberechtigt handeln zu können.
4. Welche Partei gibt so viel macht Ihren Mitgliedern bei jeder Entscheidung, bei jeder Fragestellung?